

BMXNOE0100 Firmware History

Note: Our firmware are continuously reviewed and updated in order to maintain the highest level of quality of our products. Schneider Electric recommends all customers to have their installation up to date with the newest firmware version to protect their infrastructures against cybersecurity threats and experience the best quality. For further information please visit the Schneider Electric Cybersecurity Support Portal :

<https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp>

Version #	Date of Publication	Internal reference	Description
SV3.4	11/2020	PEP0614559R VMT-1556	Resolved a TCP disconnect issue with a BMXNOE01x0 and HMIBSC. This was corrected by ensuring the six bytes of padding added to the end of the TCP frame were set to zero. CVE-2003-0001
		PEP0614560R VMT-1655	Resolved a vulnerability using the SNMPSET command that could make the device unreachable. The issue was corrected by changing the MIB variable <i>ipNetToMediaPhysAddress</i> to READ only. CVE-2020-7536
		PEP0614558R VMT-2525	Resolved a web file system access vulnerability. CVE-2020-7535
		PEP0599952R VMT-1545	Resolved a webserver GET request Denial of Service (DOS) vulnerability by detecting HTTP packets that are greater than 2048 bytes. CVE-2020-7549
		PEP0572527R	Resolved a webserver GET request Denial of Service (DOS) vulnerability by detecting HTTP packets that are not terminated.
SV3.3	01/2020	PEP0523305R	Resolved an issue where the module did not support broadcast messaging through an ethernet to serial gateway.
		PEP0614557R VMT-1719	Resolved a vulnerability to obtain information on an SMTP server configuration, including registration data of the user. CVE-2020-7533
		PEP0309446R	Resolved random occurrences of web server crashes.
		PEP0558190R	Resolved an unauthenticated Reflected XSS (Cross-site scripting) vulnerability.
		PEP0558189R	Resolved a vulnerability where a Stack Buffer Overflow results in a crash.
		PEP0558193R	Resolved an unauthenticated HTTP Password Change.
		PEP0558188R	Resolved a reboot vulnerability with an HTP script.
		PEP0558191R	Resolved an issue where any user could cause the web server to stop by sending a POST request with a zero-content length.
		PEP0558192R	Resolved a Password change vulnerability to CSRF. (Cross-site Request Forgery)
		PEP0558194R	Resolved an unauthenticated HTTP Password Reset to Default.
SV3.2	10/2017	PEP0399812R	A loss of connection would occur if both Unity and SoMove (used as an Ethernet/CANOpen gateway) were connected through the BMXNOE01x0.
		VMT-3069	Improved the coverage of web server entry methods. For further details please refer to CVE-2015-6461
SV3.1	12/2015	PEP0309176R	Removed a Remote Code Execution vulnerability in the websSecurityHandler (ICS-VU-587471)
		PEP0300706R	Removed a web server vulnerability to a remote file inclusion attack. (ICS-ALERT-15-224-02)

SV3.0	01/2015		Note: The wrong V3.0 Exec file (BMXNOE0100_v30.idx) was posted for the BMXNOE0100 on Feb 18, 2015. The correct file was posted on March 16, 2015 with the new filename (BMXNOE0100_v300.idx). Do not install the firmware with the filename BMXNOE0100_v30.idx as it could make the BMXNOE0100 inoperable and unrecoverable. The correct firmware is identified as follows: 1. The filename was changed - Correct filename BMXNOE0100_v300.idx - Incorrect filename BMXNOE0100_v30.idx 2. The .idx file sizes are different - Correct v3.00 file size: 3,102 KB - Incorrect v3.0 file size: 5,367 KB 3. If using Unity Loader: - The correct file is identified as a BMXNOE0100 V3.00 - The incorrect file is identified as a BMXNOE0110 V6.10
		PEP0259556R	There is a possibility the data in an I/O scanner message could be corrupted. The receive buffer was overwritten by an incoming message as it was being read. Interrupts are now disabled while data is being read and the issue is resolved.
		PEP0279419R	Code was corrected to restore the Graphics Viewer password button.
		PEP0271221R	Disabling FTP or HTTP in the Security tab of the Ethernet Configuration page in Unity, did not work if the PLC was reset or power cycled. At power up, the enabled/disabled state was set before the web server started. Then when the server started, the ports were enabled. Services are now disabled after the web server is started.
		PEP0273473R	The Function Block ETH-PORT-CTRL was not able to control the enable/disable state of FTP and HTTP. FTP/HTTP enable/disable bits were incorrectly implemented.
SV2.9	06/2014	PEP0228870R	Under very rare conditions, the device would not recover if power is switched on and off.
		PEP0234061R	The module experiences ARP and connection problems after 497 days of continuous operation. The 497 consecutive days powered on relates to an internal clock value within the BMXNOE0100 and is not accessible by the user. When this specific clock value is reached, the ARP cache stops updating and is no longer flushed or updated. Any connections already established would continue, but if any were closed or any new connection attempts were made, they would be refused. If the issue occurred, a reboot of the module was required to reset it. A power cycle within the 497 days would prevent the issue from occurring and reset the clock back to day 1. This can be done during any scheduled maintenance period within the 497 day time frame to avoid this event.
		PEP0241427R	Cyber Security vulnerabilities with FTP and HTTP. Option added to prevent FTP/HTTP access.
		PEP0250560R	In HTTP, using directory traversals, an attacker can bypass the basic authentication mechanism. Security Alert - ICS-VU-529542.
		PEP0251116R	Web page issue with Java Version 1.7. Files did not have security Signature. The Java dialog box provides a warning indicating that this is a unsigned application. The files all have been properly signed.
SV2.8	10/2013	OPR20051029	Daylight Savings Time 'auto' selection adjustment did not work.
		PEP0139716R	Under certain conditions, the web page may return a "Null Reference Exception" error. File fixed so the application will not return an exception when navigating from page to page.
SV2.7	01/2013		Ethernet Port Becomes Non-responsive after repeated Link Up/Down events, when it is getting its IP address through a DHCP request. There were problems with task priority handling in the DHCP. The task priorities were corrected and the link now becomes reestablished after all link-down/link-up events.

SV2.6	06/2012		If the user entered a new password as 17 characters in the http password web page, the NOE returned a page saying that the password change was successful. When the user tried use the new password, it failed. The password field was corrected to limit the user to 16 characters and no more will be accepted.
			Enhancement: Time To Live (TTL) was increased to 32.
			Changing pages very quickly causes an exception error getting returned. An incorrect function returned from the stack, combined with multiple timeout values, resulted in loss of communication resources. Function call was corrected and a single timeout replacing the previous ones resolved the issue.
			The time between READ_VAR queries increases over time if 1 or 2 of unrelated devices are disconnected. Improved handling of the Port 502 client's send message resolved the issue.
			Cyber Security services disabled and changes: 1) Removed Telnet service. 2) Removed Wind River debug service port. 3) Removed unused logins/passwords from firmware.
SV2.3	06/2011		DHCP Server did not provide Option 17 in the OFFER when it is included in the DISCOVER or REQUEST PDU's. The DHCP Server now provides the path data in all DHCP OFFERs. Option 17 is a parameter in the DHCP OFFER from the Server indicating the path of the .prm parameter file.
			A BMXNOE may not initially respond to a SYN from an XBT if both BMXNOE0100 and XBT are powered on at same time. SYN Requests are now ignored until the BMXNOE0100 is completely booted.
			BMXNOE0100 fails to recover from a serial disconnection through a Serial/Ethernet Gateway. The retransmission mechanism was modified to improve robustness against sync errors.
SV2.2	12/2010		The BMXNOE0100 may stop functioning as a DHCP Server. If the device being IO scanned has a slow response time (110-120ms), then the IO scanner was not able to open a connection. The Round Trip time algorithm for retransmission was corrected.